



United States Patent and Trademark Office



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/430,879	11/01/1999	ROBERT ZUCCHERATO	0500.9906161	7876
7590 11/04/2003			EXAMINER	
MARKISON & RECKAMP PC			SMITHERS, MATTHEW	
PO BOX 06229			ART UNIT	PAPER NUMBER
WACKER DRIVE CHICAGO, IL 60606			2134	

DATE MAILED: 11/04/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

<u> </u>		Application No.	Applicant(s)			
•		09/430,879	ZUCCHERATO ET AL.			
	Office Action Summary	Examiner	Art Unit			
	•	Matthew B Smithers	2134			
	- The MAILING DATE of this communication app	pears on the cover sheet with the	correspondence address			
Period fo	r Reply					
THE N - Exten after t - If the - If NO - Failur - Any re earne	DRTENED STATUTORY PERIOD FOR REPL' MAILING DATE OF THIS COMMUNICATION. sions of time may be available under the provisions of 37 CFR 1.1 SIX (6) MONTHS from the mailing date of this communication. period for reply specified above is less than thirty (30) days, a repl period for reply is specified above, the maximum statutory period e to reply within the set or extended period for reply will, by statute eply received by the Office later than three months after the mailing d patent term adjustment. See 37 CFR 1.704(b).	I36(a). In no event, however, may a reply be ly within the statutory minimum of thirty (30) d will apply and will expire SIX (6) MONTHS fro	timely filed lays will be considered timely. om the mailing date of this communication. NED (35 U.S.C. § 133).			
Status	Responsive to communication(s) filed on <u>01</u>	November 1999				
1)⊠	<u> </u>	his action is non-final.				
2a)☐	This action is FINAL . 2b)⊠ The Since this application is in condition for allow		prosecution as to the merits is			
3)	closed in accordance with the practice under	Ex parte Quayle, 1935 C.D. 11	, 453 O.G. 213.			
-	on of Claims		•			
•	Claim(s) 1-35 is/are pending in the applicatio					
	4a) Of the above claim(s) is/are withdra	awn from consideration.				
•	Claim(s) is/are allowed.					
	Claim(s) <u>1-5,7-31 and 33-35</u> is/are rejected.					
	Claim(s) <u>6 and 32</u> is/are objected to.					
	Claim(s) are subject to restriction and/	or election requirement.				
• •	ion Papers	or				
	The specification is objected to by the Examinon The drawing(s) filed on is/are: a)□ acce		xaminer.			
10)	Applicant may not request that any objection to the	he drawing(s) be held in abevance.	See 37 CFR 1.85(a).			
111	The proposed drawing correction filed on	is: a) ☐ approved b) ☐ disap	proved by the Examiner.			
ווי י	If approved, corrected drawings are required in re					
12)□	The oath or declaration is objected to by the E					
•	under 35 U.S.C. §§ 119 and 120					
_	Acknowledgment is made of a claim for foreig	gn priority under 35 U.S.C. § 11	9(a)-(d) or (f).			
	a) ☐ All b) ☐ Some * c) ☐ None of:					
۵,	1. Certified copies of the priority documents have been received.					
	2. Certified copies of the priority documents have been received in Application No					
	3 Copies of the certified copies of the priority documents have been received in this National Stage					
	application from the International B See the attached detailed Office action for a lis	Bureau (PC1 Rule 17.2(a)). st of the certified copies not rece	eived.			
	Acknowledgment is made of a claim for domes					
15)□	 a) The translation of the foreign language p Acknowledgment is made of a claim for dome. 	rovisional application has been stic priority under 35 U.S.C. §§	received. 120 and/or 121.			
Attachme	nt(s)	_				
2) X Noti	ce of References Cited (PTO-892) ce of Draftsperson's Patent Drawing Review (PTO-948) rmation Disclosure Statement(s) (PTO-1449) Paper No(s)	5) Notice of Inform	mary (PTO-413) Paper No(s) nal Patent Application (PTO-152)			
L						

Application/Control Number: 09/430,879

Art Unit: 2134

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed November 1, 1999 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 7-31 and 33-35 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. patent 4,783,798 granted to Leibholz et al.

Regarding claim 1, Leibholz meets the claimed limitations as follows:

"A method for initializing operation for an information security operation for an entity comprising the steps of:

obtaining data representing entity identification data;

obtaining data representing shared data associated with the entity identification data;

encrypting data, based on the shared data; communicating in a clear text fashion, the entity identification data and the encrypted data for evaluation by an initialization authentication unit;

Application/Control Number: 09/430,879

Art Unit: 2134

comparing prestored shared data to shared data derived from the encrypted data to obtain the entity identification data; and using the obtained entity identification data and the shared data as initialization registration data to register the entity as a proper user of the information security operation, in response to the step of comparing prestored shared data to shared data derived from the encrypted data." see column 5, line 57 to column 9, line 34.

Regarding claim 2, Leibholz meets the claimed limitations as follows:

"The method of claim 1 wherein the data that is encrypted includes data representing the entity identification data." see column 6, lines 4-10.

Regarding claim 3, Leibholz meets the claimed limitations as follows: "The method of claim 1 wherein the data that is encrypted includes temporal data." see column 6, lines 4-10.

Regarding claim 4, Leibholz meets the claimed limitations as follows:

"The method of claim 2 including the step of generating first data that is a function of the entity identification data, and wherein the step of encrypting data includes encrypting the first data based on the shared data." see column 6, lines 4-10.

Regarding claim 5, Leibholz meets the claimed limitations as follows:

"The method of claim 4 including the step of generating second data that is a function of the shared data, and wherein the step of encrypting data includes encrypting the first data based on the second data." see column 8, lines 39-55.

Regarding claim 7, Leibholz meets the claimed limitations as follows: "The method of claim 1 including the step of:

Application/Control Number: 09/430,879

Art Unit: 2134

prestoring the data representing the entity identification data and pre-storing the shared data, prior to the steps of obtaining." see column 6, lines 4-10 and column 6, line 52 to column 7, line 17.

Regarding claim 8, Leibholz meets the claimed limitations as follows:

"The method of claim 7 including the steps of generating first data that is a function of the prestored data representing the entity identification data; storing the first data with the prestored shared data as database entries; extracting from a database entry, the prestored shared data based on the first data; generating second data as a function of the extracted prestored shared data; and providing the second data for use in the step of comparing." see column 6, lines 4-10 and column 6, line 52 to column 7, line 17.

Regarding claim 9, Leibholz meets the claimed limitations as follows:

"The method of claim 1 wherein the shared data is shared secret data." see column 6,
lines 4-10.

Regarding claim 10, Leibholz meets the claimed limitations as follows: "The method of claim 8 including the step of prior to the step of comparing, decrypting, by the initialization authentication unit, the encrypted data using the second data." see column 6, lines 4-10 and column 6, line 52 to column 7, line 17.

Regarding claim 11, Leibholz meets the claimed limitations as follows: "The method of claim 1 wherein steps of comparing prestored shared data to shared data derived from the encrypted data includes comparing data derived from the prestored shared data to data derived from the shared data." see column 6, line 52 to column 7, line 17.

Regarding claim 12, Leibholz meets the claimed limitations as follows:

"A method for initializing operation for an information security operation for an entity comprising the steps of:

obtaining pre-stored data representing entity identification data;

obtaining pre-stored data representing shared secret data associated with the entity identification data;

generating first data that is a function of the entity identification data, generating second data that is a function of the shared secret data, encrypting the first data based on the second data;

communicating in a clear text fashion, the entity identification data and the encrypted first data for evaluation by an initialization authentication unit;

generating a copy of the first data as a function of the prestored data representing the entity identification data; storing the copy of the first data with the prestored shared secret data as database entries;

extracting from a database entry, the prestored shared secret data based on communicated first data;

generating a copy of the second data as a function of the extracted prestored shared secret data;

providing the copy of the second data for use in comparing pre-stored shared secret data to shared secret data derived from the encrypted first data to obtain the entity identification data; and using the obtained entity identification data and the shared secret data as initialization registration data to register the entity as a proper user of the

Art Unit: 2134

information security operation, in response to the step of comparing data derived from pre-stored shared secret data to shared secret data derived from the encrypted data." see column 5, line 57 to column 9, line 34.

Regarding claim 13, Leibholz meets the claimed limitations as follows: "The method of claim 12 wherein the pre-stored data representing entity identification data includes temporal data." see column 6, lines 4-10.

Regarding claim 14, Leibholz meets the claimed limitations as follows: "The method of claim 12 wherein the first data and second data are generated using a function from the group consisting of: a one way hash function, SPEKE, a block cipher encryption, a MAC, a public key encryption, or the identity function." see column 8, lines 20-51.

Regarding claim 15, Leibholz meets the claimed limitations as follows: "The method of claim 12 including the step of prior to the step of comparing, decrypting, by the initialization authentication unit, the encrypted first data using the second data based on the database entry." see column 6, line 52 to column 7, line 17. Claims 16-20, 22-23 and 25-26 are system claims that are substantially equivalent to method claims 1-5 and 7-11. Therefore claims 16-20, 22-23 and 25-26 are rejected by a similar rationale.

Regarding claim 21, Leibholz meets the claimed limitations as follows: "The system of claim 19 wherein the first data and second data are generated using a function from the group consisting of a one way hash function, SPEKE, block cipher

Art Unit: 2134

encryption, a MAC, public key encryption, or the identity function." see column 8, lines 20-51.

Regarding claim 24, Leibholz meets the claimed limitations as follows: "The system of claim 22 wherein the initialization authentication unit includes the second processor." see column 5, lines 39-41.

Claims 27-31 and 33-35 are computer readable medium claims that are substantially equivalent to method claims 1-5 and 7-9. Therefore claims 27-31 and 33-35 are rejected by a similar rationale.

Allowable Subject Matter

Claims 6 and 32 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 6 and 32, the cited prior art fails to specifically teach wherein the first data and second data are generated using a function from the group consisting of a one way hash function and PAKE.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

* Application/Control Number: 09/430,879

Art Unit: 2134

A. Matyas (4,771,461) discloses a method for initializing cryptographic variables in an electronic transaction network.

B. Wood et al (6,609,198) discloses a secure log-on service allowing change in a credential without losing the continuity of a session.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B Smithers Primary Examiner Art Unit 2134